PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, 12/14 — A1

(11) International Publication Number: WO 95/22793

(43) International Publication Date: 24 August 1995 (24.08.95)

(21) International Application Number: PCT/US95/01740

(22) International Filing Date: 9 February 1995 (09.02.95)

(30) Priority Data:
08/198,745 18 February 1994 (18.02.94) US

(71) Applicant: INFOSAFE SYSTEMS, INC. [US/US]; Suite 622, 342 Madison Avenue, New York, NY 10173 (US).

(72) Inventors: NAGEL, Robert; Suite 7F, 33 Riverside Drive, New York, NY 10023 (US). LIPSCOMB, Thomas, H.; 145 East 74th Street, New York, NY 10021 (US).

(74) Agent: MILDE, Karl, F., Jr.; Karl F. Milde, Jr., P.C., Suite 210, 2 Crosfield Avenue, West Nyack, NY 10994 (US).

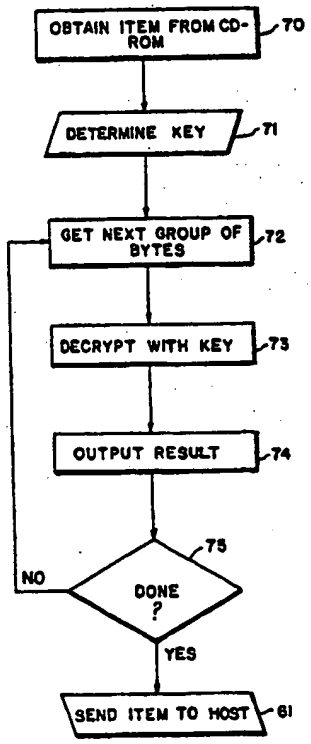
(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, UG, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: APPARATUS AND STORAGE MEDIUM FOR DECRYPTING INFORMATION

(57) Abstract

A system including a storage medium containing encrypted information comprises: (a) a control unit for selecting information to be retrieved from the storage medium; (b) a storage medium reader for reading the selected information from the storage medium; and (c) a decryption device for decrypting at least portions of the selected information using a decryption key. The decryption key is defined, at least in part, by rules and/or data which are read from the storage medium by the storage medium reader. A different and unique key is associated with each separate item or file of encrypted information.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

APPARATUS AND STORAGE MEDIUM FOR DECRYPTING INFORMATION

BACKGROUND OF THE INVENTION

The present invention relates to a system (apparatus), and a storage medium, for retrieving secure information from a local database for temporary storage, printing and usage by an information user.

Systems for storage and retrieval of secure information are well known in the art. As used herein, the term "secure information" is intended to mean information (alphanumeric data, graphics and the like) which is either encrypted or otherwise protected to prevent access thereto except by an authorized user. Such systems have been proposed and are employed both for the case where the information source (database) is centralized, and for the case where the information source has been distributed to multiple users. In the latter case, CD-ROMs have been used to export databases to multiple users so that information storage and retrieval takes place at the user site.

In the U.S. Patent No. 5,010,571 to Ron Katznelson and the U.S. Patents Nos. 4,827,508, 4,977,594 and 5,050,213 to Victor Shear, it is proposed to provide encrypted digital information on CD-ROMs at the user site and to monitor and account for each item or "packet" of information which is retrieved and decrypted from a CD-ROM by an authorized user.

This concept of retrieving information on a "pay-as-you-go" basis is also disclosed in the U.S. Patent No.

5,247,575 of Peter J. Sprague and Thomas H. Lipscomb to include individual access to encrypted data which is "broadcast" to multiple user sites from a central source and/or to provide individual access to encrypted data stored at a central source, using conventional time sharing techniques and transmission via telephone dial-up or local area network (LAN) or wide area network (WAN) communication.

All of these prior art systems permit the user's access to the secure information to be monitored and strictly controlled. This is accomplished, in practice, by maintaining a record at each user site of each information packet that is retrieved as well as the cost thereof to the user, and then "polling" all user sites from a remote central site, on a regular basis, to retrieve the user data and, if necessary, disable the equipment at one or more user sites to prevent further access to the secure information at these sites.

Systems of the type require a confidential "decryption key" to enable the decryption of the encrypted information using a standard or a specialized decryption algorithm. As used herein, the term "decryption key" or simply "key" is intended to mean a series of numbers or characters which, when utilized in a decryption algorithm, decrypts encrypted data.

In the aforementioned patents it has been proposed to transmit these keys to each user site on a regular basis,

provided that the user's financial account is up-to-date. If a user workstation does not receive a new key before the previous key expires, the ability of the workstation to decrypt information from CD-ROMs will terminate.

Needless to say, transmitting new keys to each user workstation, even at six month intervals, is a time consuming task and such transmission is subject to interception and attack by persons who would attempt to obtain free and unfettered access to the encrypted information.

Furthermore, the use of a single key to gain access to all encrypted information on one or more CD-ROMs is fraught with danger. If this single key were discovered or "reverse engineered", all encrypted information on the CD-ROM's would become available to persons who may have no intention of paying for it.

SUMMARY OF THE INVENTION

It is accordingly an object of the present invention to provide a system for decryption of encrypted information which does not require that decryption keys be transmitted from one place to another.

It is a further object of the present invention to provide a system for decrypting encrypted information which utilizes different keys for different segments of information.

It is a further object of the present invention to disable a system for decryption of encrypted information if a user thereof is no longer authorized to retrieve information from storage.

These objects, as well as further objects which will become apparent from the discussion that follows, are achieved, in accordance with the present invention, by providing a system wherein at least one decryption key is associated with each storage medium (e.g., CD-ROM) for decryption of information thereon, and wherein each key is defined, at least in part, by data stored on the storage medium.

In a preferred embodiment of the present invention, there is provided a system which comprises:

(a) a control unit for selecting information to be retrieved from the storage medium;

(b) a storage medium reader for reading the selected information from the storage medium; and

(c) a decryption device for decrypting at least portions of the selected information.

The decryption key is defined, at least in part, by data which are read from the storage medium by the storage medium reader.

In a preferred embodiment of the invention, the decryption key "K" is defined by "key rules" and by "key data" applied to the key rules. For example, a single key

rule might be "K = two's complement of X" where the key data is "X". In this case, the key K may be changed by either changing the key rule, by changing the key data or by changing both the key rule and the key data. The portion of the key rules and key data which are stored on the storage medium, or are otherwise obtained locally, will hereinafter be termed a "key message".

According to a preferred feature of the present invention, the information stored of the storage medium is divided into separate marketable segments and each segment has associated therewith a different and unique decryption key. Preferably also, the key message for each segment is defined, at least in part, by data contained in the respective segment on the storage medium.

For example, the storage medium may have stored thereon a plurality of separate, content-defined files of information. In this case, the segments of information are preferably these separate files of information.

In the latter case, the storage medium may have stored thereon a "file directory" containing the identity, length, location and date of each file. In this case, the key message for each file is preferably defined, at least in part, by information contained in the file directory.

According to another preferred feature of the present invention, the storage medium has stored thereon a "media message" containing information unique to this storage

medium, such as the CD-ROM header if the storage medium is a CD-ROM. In this case, the key message for each file is defined, at least in part, by information contained in this media message.

As a further option, the system for retrieving information may include a real time clock for providing the current date and time. In this case, the key message may be defined, at least in part, by the current date and time.

As a still further option, the system for retrieving information may comprise an input device for providing a "communication message" to the decryption controller. Such an input device may, for example, be a telephone modem capable of receiving data over the telephone network from a remote, central source. In this case, the key message may be defined, at least in part, by this communication message.

In prior information distribution systems, such as those disclosed in the U.S. patents referred to above, it has been the practice to disable the decryption of information at the user site by one of three methods: (1) sending a "disable" signal to a user station; (2) allowing a user station to disable itself when the prepaid credit for information has been used up; and (3) not sending a new decryption key when the period for use of the prior key has lapsed. In accordance with a preferred feature of the present invention, user stations are also disabled automatically if they have not received a telephone call,

via modem, within a prescribed length of time. This length of time can be set to a default value, so that the station is automatically disabled if it is moved from its customary place and does not receive a telephone call. The prescribed length of time may also be set by information contained in a telephone call to change this default time to a shorter time period, if desired. In this way, if the decrypting device is stolen, it will automatically disable itself after 24 hours, for example, even though the authorized user may have a large prepaid balance in the financial account.

As a further security, the system will automatically disable itself when it is tampered with; that is, when an unauthorized person attempts to open and remove the unit's enclosure. This feature is preferably implemented by provided light-sensitive programmable elements containing programs that are erased upon the receipt of light.

For a full understanding of the present invention, reference should now be made to the following detailed description of the preferred embodiments of the invention as illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a representative diagram of a workstation comprising a personal computer (PC), a CD-ROM reader and a decryption controller all arranged on an SCSI bus.

Fig. 2 is a block diagram of a decryption controller for use in the system of Fig. 1.

Fig. 3 is a flow chart showing the general operation of the decryption controller of Fig. 2.

Fig. 4 is a flow chart showing the general operation of the decryption controller of Fig. 2 in response to an SCSI command from the host computer.

Fig. 5 is a flow chart showing the general operation of the decryption controller in response to an SCSI command to retrieve an item of information.

Fig. 6 is a flow chart showing the operation of the decryption controller in decrypting data.

Fig. 7 is a flow chart showing the operation of the decryption controller in creating a decryption key.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The preferred embodiments of the present invention will now be described with reference to Figs. 1-7 of the drawings. Identical elements in the various figures are designated with the same reference numerals.

Fig. 1 illustrates the general nature of the system according to the present invention. As shown here, the system involves a digital computer workstation which is capable of retrieving secure data from a database stored on one or more CD-ROMs.

In order to prevent unauthorized access to the stored information, at least some of the individual items of information ("information packets") are encrypted prior to storage on a CD-ROM. Some of the information packets may also be stored in decrypted (cleartext) form on a CD-ROM and can be retrieved by any workstation user by means of a CD-ROM reader. However, only an authorized user with a proper validated code is allowed to decrypt the encrypted information packets.

Upon release of the secure and, if desired, the non-secure information to an authorized user, the user is charged a preset fee set by the information provider (copyright owner or publisher of the information). This charge is effected automatically by debiting a financial account which has previously been established between the user and the information provider.

To implement this system, there is provided a workstation comprising a personal computer (PC) 10, a CD-ROM reader 12 and a decryption controller 14. These three devices, which may be stand-alone devices each arranged in a separate enclosure or combined in one or two enclosures -- e.g., the PC 10 in one enclosure and the CD-ROM reader 12 and controller 14 in another -- are connected in a well-known manner to a Small Computer System Interface ("SCSI") bus 16 via a bus interface and controller 18.

The personal computer 10 and the CD-ROM reader 12 are conventional devices which are available commercially. The decryption controller is a special purpose device which operates to receive encrypted data from the CD-ROM reader, decrypt this data if authorized to do so, and transport the decrypted data to the host computer 10 for storage either in its active memory (RAM) or hard disk drive.

The decryption controller also keeps a running account of the identity of, and charge for each information packet which is decrypted for later transmission, e.g. by telephone line, to a central billing facility at a remote site. A monitoring facility of this type is known from the aforementioned U.S. Patents Nos. 5,010,571; 4,827,5089 and 5,247,575.

Once an information packet is decrypted and transferred to the host computer 10, the workstation user can display it on the computer screen, print out a hard copy and/or transmit a copy by LAN or modem to another workstation.

In accordance with the SCSI standard, the SCSI bus extends no more than twenty-six feet in length from end to end and is provided with terminating impedances at each end. Each unit arranged on the bus is provided with a unique address from a maximum of eight addresses (zero to seven). The computer is usually given the address number seven; the addresses of the other devices on the bus may be selected

from zero to seven with a manual switch arranged on each device.

In the preferred embodiment of the present invention, the decryption controller 14 is disposed in its own enclosure, separate and apart from the personal computer 10 and possibly also the CD-ROM reader 12. To safeguard the firmware and codes which are used by the electronic circuitry, the decryption controller may be provided with light-sensitive, erasable memory circuits so that the contents of memory are erased if and when the enclosure is opened.

Fig. 2 shows a preferred embodiment of the decryption controller. This device is connected to the SCSI bus 16 via receptacles 20 and a fifty pin header 22. The SCSI bus controller 18 operates in conjunction with a CPU 24 to receive requests for data from the host computer 10 and initiate requests for this data from the CD-ROM reader 12.

The device is provided with its own separate power supply 26 so that it operates completely independently of the host computer 10.

The decryption controller is also provided with a 2400 baud modem and telephone interface 28 so that it may communicate with a central billing computer at a remote site. This central billing computer routinely calls the decryption controller 18 at regular intervals -- for example, each night -- to download the logged information

concerning each information packet (IP) that was decrypted, and/or to credit the financial account maintained by the decryption controller when the workstation user makes payment.

The decryption controller 18 can also communicate with other devices, such as printers or the like, by means of an RS-232C transceiver 30 and an associated serial port connector 32.

The SCSI address is set from zero to six by a manual ID selector 34. Date and time are provided by a real time clock 36.

Firmware for the decryption controller is provided on two 128K flash memory chips 38; intermediate scratch pad storage is provided by a 256K dynamic RAM 40.

Decryption of encrypted data is effected by a Data Encryption Standard (DES) module 42 which operates in conjunction with a key code scrambler 44. The key code scrambler maintains the keys used by the DES module for decryption. Alternatively, the decryption function and/or the key code scrambler function may be implemented in software (firmware) operating in the CPU 24.

All keys utilized by the system are created and maintained in the decryption controller so that neither the workstation user nor the PC 10 will have access to these keys.

All of the electronic circuit devices contained in the decryption controller of Fig. 2 are standard, commercially available devices. Part numbers are shown in Fig. 2 for the major components.

In a preferred embodiment of the invention, the system of Fig. 1 and, in particular, the decryption controller of Fig. 2, operates in the manner shown by the flow charts of Fig. 3-7.

When first switched on, the CPU 24 executes a self-test routine as is conventional in the art (Block 45 in Fig. 3). Error messages are communicated to the host computer via the SCSI bus for display to the system user. Thereafter, the CPU enters the idle mode (Block 46) and awaits an interrupt.

If the decryption controller receives an SCSI command from the host computer (Block 47) it processes this command (Block 48) as will be described hereinafter in connection with Fig. 4. If the decryption controller receives an incoming telephone message (Block 49) from a central billing computer, it processes this message (Block 50) before proceeding. Typical telephone messages are set forth in Table I:

TABLE I

Set Credit (in financial account)
Set Item Price
Set User Password
Clear Financial Account to Zero
Get Financial Account Information
Get User Information
Create User Information
Remove User Information
Send User a Message

Similarly, if an RS232 connection is established (Block 51), permitting communication either to or from the decryption controller, the controller either transmits information, for example to a printer, or receives a serial message of the type noted above. In this case, the serial message is processed (Block 52) and the controller returns to the idle state.

Fig. 4 illustrates how an SCSI command from the host computer is treated by the decryption controller. When an SCSI command is received (Block 53) it is analyzed and processed (Block 54) by the decryption controller. Typical SCSI commands are set forth in Table II:

TABLE II

Get Financial Account Information
Get Purchased Item Information
Assent/Don't Assent to Purchase Item
Log In
Log Out
Poll for an Asynchronous Event (such as an "on sale" notice)
Set User's Default Billing Reference (e.g., last billing reference number used)
Purchase Item
Get Decryption Controller Status (i.e., error codes)
Get User Information (i.e., currently logged-in user)
Receive Decrypted Data

Certain PC commands require the decryption controller to call the central billing computer via the telephone modem. For example, if the financial account is decremented to zero, the decryption controller will automatically call and request additional credit. In this case, the decryption controller makes the call (Block 55) and executes the call-

out sequence (Block 56). In the call-out protocol, the decryption controller dials the number of the central billing facility and transmits both its telephone and identification (ID) numbers. This simple transmission requests an immediate call-back from the central computer during which the financial account is automatically updated.

Each telephone transaction, initiated by the central billing computer, preferably comprises three steps:

(1) A download to the central billing facility of the current financial account status, all billing transactions completed since the previous download, and the user information stored in the decryption controller;

(2) A transmission from the central billing facility to the decryption controller of any updates, such as changes in pricing information and the like; and

(3) A communication of all error codes from the decryption controller to the central billing facility which indicate that the decryption controller is not functioning properly.

In addition, the financial account balance in the decryption controller can be updated by the central billing facility. It can be credited, if payment was made to the central billing facility by the user, or debited, for example if a check was returned from the bank marked "insufficient funds".

Each billing transaction provided to the central billing facility preferably contains, at a minimum, the following information:

Time and Date of Decryption
Identification No. of Information Packet (IP)
Volume No. of CD-ROM
Information Owner or Distributor of IP
Type of IP (Classification)
Price Paid for IP
Billing Reference, if inserted by the User

When an item (IP) is purchased by a user, and the decryption controller is able to complete this transaction by decrementing the financial account and decrypting the item, this transaction is logged into the flash memory 38 of the controller. In this case, the logging operation is flagged (Block 57) and carried out (Block 58) at the completion of the transaction. Thereafter, the decryption controller returns to the idle mode (Block 59).

Referring to Fig. 5, the retrieval of an item (IP) commences with a request by the host computer 10 (Block 60). The host computer sends this request to the decryption controller 14 via the SCSI bus which processes the request and then sends the item to the host (Block 61), as if it were the CD-ROM reader. The host computer 10 thus addresses the decryption controller, rather than the CD-ROM reader; however, with the exception of this difference, the host computer operates in such a manner as if it were requesting the item of data directly from the CD-ROM reader. Thus, as far as the host computer 10 is concerned, the decryption

controller is the CD-ROM reader; i.e., it is indistinguishable from, and "transparent' to the host computer.

The decryption controller initially queries the file directory of the CD-ROM to determine whether the item of information is encrypted (Block 62). If not, the decryption controller initiates a data request from the CD-ROM reader 12 (Block 63) in the same manner as if it were the host computer and reads the item into its own RAM memory. Thereafter, the data item is transferred to the host computer (Block 61).

If the file directory indicates that the desired item is encrypted, the decryption controller checks the user's financial account to determine if there is a sufficient positive balance to pay for the item (Block 64). If not, the decryption controller informs the host computer of the insufficient credit (Block 65).

If credit is sufficient, the decryption controller transmits the cost of the item to the host computer and asks the host to confirm the purchase (Block 66) by displaying the cost to the user and requesting a user response. If the user fails to accept the purchase, the transaction is terminated (Block 67).

If the host computer confirms the purchase of the item at the price indicated, the decryption controller initiates a data request to the CD-ROM reader. The item is thus

caused to be read by the CD-ROM reader and it is transferred to the RAM of the decryption controller. Thereafter, the item is decrypted using the DES module and the decryption keys (Block 68). The purchase price of the item is then debited from the user's financial account (Block 69) and the decrypted item is transferred to the host computer (Block 61). Once the item of information has been supplied to the host computer in decrypted form, it is available for storage, both temporary and archival storage, and may be read and copied by the user, as desired.

Fig. 6 illustrates the detailed operation of the decryption controller of Fig. 2 in decrypting an item of information. As such, Fig. 6 represents the operation of Block 68 in Fig. 5.

As an initial step, the controller obtains the entire item of information (in encrypted form) from the CD-ROM (Block 70). Thereafter, the controller determines the decryption key (Block 71) for this item from key rules and key data which are available (e.g., stored) locally. Preferably, each separate item of information has a unique decryption key. The method of determining the key will be described in detail hereinafter in connection with Fig. 7.

Since the DES module 42 of the decryption controller processes (decrypts) only eight bytes of data at a time, a first group of eight bytes for the information item to be decrypted is initially transferred to the DES circuit (Block

72) and decrypted (Block 73). The result of this decryption -- that is, the cleartext -- is placed temporarily in RAM (Block 74) and the process is repeated (Block 75) until all bytes of data of the information item are decrypted. Thereafter, the entire information item in cleartext is transmitted to the host computer (Block 61).

Fig. 7 illustrates how the decryption key is determined from the key rules and the key data which are available locally for each separate item of information stored on the CD-ROM. In order to determine the key, it is necessary to obtain both the key rules and the key data for the specific item of information, and then to apply the rules to this data. Examples of both rules and data are given below.

The key rules and the key data are preferably obtained from one or more of the following five sources:

(1) Non-volatile storage of a "system message" within the decryption controller (flash memory);

(2) A "communication message" received from either the host computer, via the SCSI bus or RS232C interface, or the central billing facility via the telephone modem;

(3) A "media message" contained on the CD-ROM header which is generic to all the files stored thereon (for example, the volume number of the CD-ROM);

(4) A "file message" constructed from information on the file directory associated with the specific item of information (IP) to be decrypted (for example, the identity,

length, location and date of the respective file) and/or the header portion of the IP itself; and

(5) A "current status message" obtained from some element of the decryption controller (for example, the real time clock) or the host computer.

Referring to Fig. 7, it is seen that a "key message" -- that is, the key rules and key data for generating a key -- is obtained by retrieving a stored system message (Block 80), by retrieving a stored communication message (Block 81), by reading the media message from the CD-ROM (Block 82), by reading the file directory and header of the selected IP from the CD-ROM (Block 83), and by obtaining the current status of the decryption controller (Block 84). With this information, all of which is available locally at the user site, the key rules and key data are selected (Block 85). Thereafter, the key data is applied to the key rules (Block 86) to produce the decryption key.

By way of example and not limitation, the following key rules are suggested:

(1) Add the CD-ROM volume number from the media message to the length of the IP from the file message.

(2) Add the date from the media message to the date from the file message.

(3) Add the most recent communication message (initial vector) to the file location in the file message.

(4) Subtract the date found in the file message (date of creation of the IP) from the current status (present date). If the result is positive and less than one year, proceed to decrypt. If the result is negative or more than one year, do not generate a key (do not decrypt).

Other combinations of key rules and key data will readily occur to those skilled in the art.

There has thus been shown and described a novel apparatus and storage medium for decrypting information which fulfills all the objects and advantages sought therefor. Many changes, modifications, variations and other uses and applications of the subject invention will, however, become apparent to those skilled in the art after considering this specification and the accompanying drawings which disclose the preferred embodiments thereof. All such changes, modifications, variations and other uses and applications which do not depart from the spirit and scope of the invention are deemed to be covered by the invention, which is to be limited only by the claims which follow.

C L A I M S

What is claimed is:

1. In apparatus for retrieving information from a readable storage medium, at least some of which information is stored on said medium in encrypted form and may be decrypted using a decryption algorithm which requires a decryption key, wherein said apparatus comprises:

(a) a storage medium for storing information;

(b) a control unit for selecting information to be retrieved from said storage medium;

(c) a storage medium reader for reading said selected information from said storage medium; and

(d) a decryption device for decrypting at least portions of said selected information;

the improvement wherein at least one decryption key is associated with said storage medium for decryption of said selected information, and wherein said decryption key is defined, at least in part, by data stored on said storage medium.

2. The apparatus defined in claim 1, wherein said decryption key is defined by key rules and by key data applied to said key rules, and wherein a key message comprising at least one of said key rules and said key data is stored on said storage medium.

3. The apparatus defined in claim 1, wherein said information stored on said storage medium is divided into segments; wherein each segment has associated therewith a different and unique decryption key.

4. The apparatus defined in claim 3, wherein said storage medium has stored thereon a plurality of separate, content-defined files of information and wherein said segments of information are said files of information.

5. The apparatus defined in claim 4, wherein said storage medium is a CD-ROM having a plurality of storage blocks and wherein said files of information are the information stored in said separate storage blocks on said CD-ROM.

6. The apparatus defined in claim 4, wherein said decryption key is defined by key data and by key rules applied to said key data, and wherein a key message comprising at least one of said key rules and said key data is stored on said storage medium.

7. The apparatus defined in claim 6, wherein said storage medium has stored thereon a file directory containing the identity, length, location and date of each file, and wherein the key message for each file is defined

at least in part, by information contained in said file directory.

8. The apparatus defined in claim 7, wherein said key message for a particular file is defined by data selected from the group consisting of the identity, length, location and date of the respective file contained in said file directory.

9. The apparatus defined in claim 6, wherein said storage medium has stored thereon a media message containing information unique to the storage medium, and wherein the key message for each file is defined, at least in part, by information contained in said media message.

10. The apparatus defined in claim 6, further comprising a real time clock for providing the current date and time, and wherein said key message is defined, at least in part, by said current date and time.

11. The apparatus defined in claim 6, further comprising an input device for providing a communication message, and wherein said key message is defined, at least in part, by said communication message.

12. The apparatus defined in claim 3, wherein said decryption key for each segment is defined, at least in part, by data stored in the respective segment on said storage medium.

13. In a storage medium having stored thereon a plurality of files of information, at least some of which files contain encrypted information;

the improvement wherein each file containing encrypted information has associated therewith a separate and unigue decryption key which is required for the decryption of the encrypted file information.

14. The storage medium defined in claim 13, wherein said decryption key is defined by key data and by key rules applied to said key data, and wherein a key message comprising at least one of said key rules and said key data is stored on said storage medium.

15. The storage medium defined in claim 14, having further stored thereon a file directory containing the identity, length and location of each file, and wherein the decryption key for each file is defined, at least in part, by the information relevant to such file which is contained in said file directory.

16. The storage medium defined in claim 14, wherein said key message for a particular file is defined by data selected from the group consisting of the identity, length, location and date of the respective file contained in said file directory.

17. The storage medium defined in claim 14, wherein said storage medium has stored thereon a media message containing information unique to the storage medium, and wherein the key message for each file is defined, at least in part, by information contained in said media message.

18. The storage medium defined in claim 13, wherein said storage medium is a CD-ROM having a plurality of storage blocks and wherein said files of information are the information stored in said separate storage blocks on said CD-ROM.

19. In apparatus for retrieving information from a readable storage medium, at least some of which information is stored on said medium in encrypted form and may be decrypted using a decryption algorithm which requires a decryption key, wherein said apparatus comprises:

(a) a storage medium for storing information;

(b) a control unit for selecting information to be retrieved from said storage medium;

(c) a storage medium reader for reading said selected information from said storage medium;

(d) a decryption device for decrypting at least portions of said selected information; and

(e) a telephone modem for receiving telephone messages via the telephone network from a remote source,

the improvement comprising disabling means, coupled to said telephone modem, for disabling said decryption device from decrypting information at a prescribed moment of time unless reset by the receipt of a telephone message.

20. The apparatus defined in claim 19, wherein said disabling means is operative to disable said decryption means upon expiration of a given length of time after receipt of a prior telephone message.

21. The apparatus defined in claim 20, wherein said given length of time is included in said prior telephone message.

22. In apparatus for retrieving information from a readable storage medium, at least some of which information is stored on said medium in encrypted form and may be decrypted using a decryption algorithm which requires a decryption key, wherein said apparatus comprises:

(a) a storage medium for storing information;

(b) a control unit for selecting information to be retrieved from said storage medium;

(c) a storage medium reader for reading said selected information from said storage medium; and

(d) a decryption device for decrypting at least portions of said selected information, said decryption device having an enclosure to inhibit access thereto by unauthorized personnel;

the improvement comprising disabling means for disabling said decryption device from decrypting information when said enclosure is removed.

23. The apparatus defined in claim 22, wherein said disabling means includes a light-sensitive programmable element for storing a program, said programmable element being operative to erase the stored program upon the receipt of light.

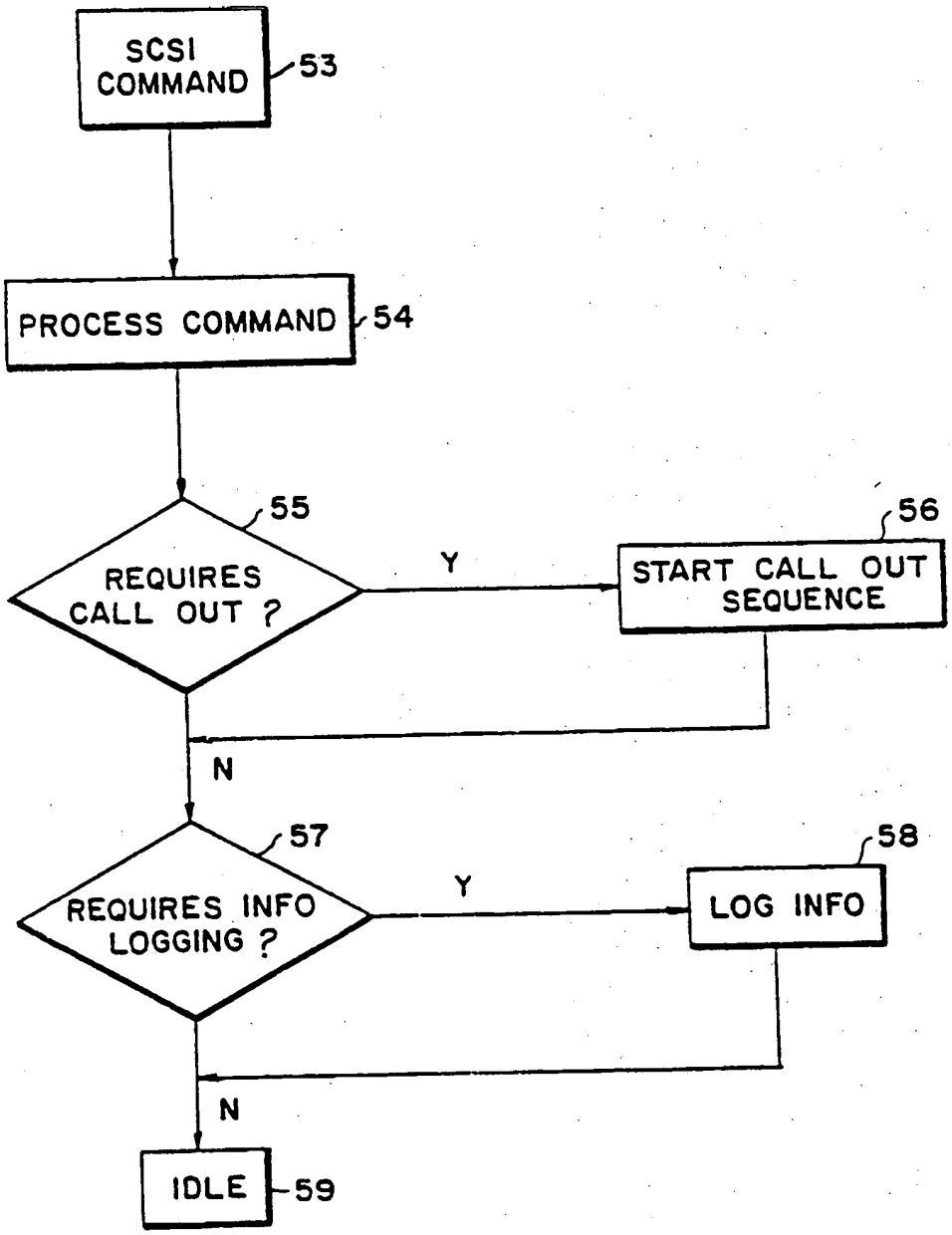

SCSI COMMAND
53
PROCESS COMMAND
54
55
REQUIRES CALL OUT ?
Y
56
START CALL OUT SEQUENCE
N
57
REQUIRES INFO LOGGING ?
Y
58
LOG INFO
N
IDLE
59

FIG.4

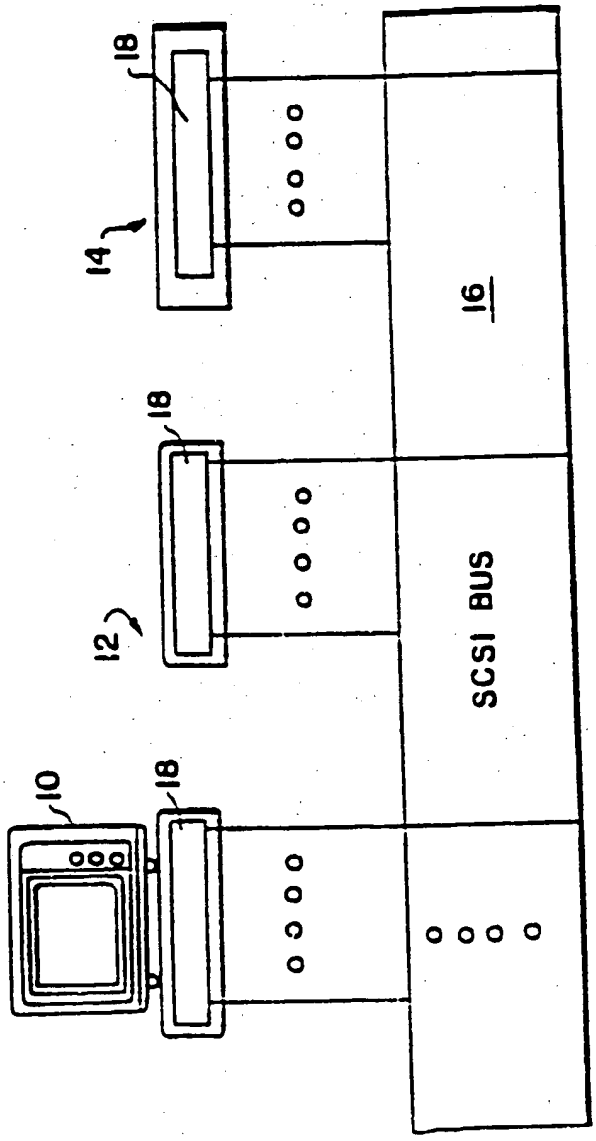


FIG.1

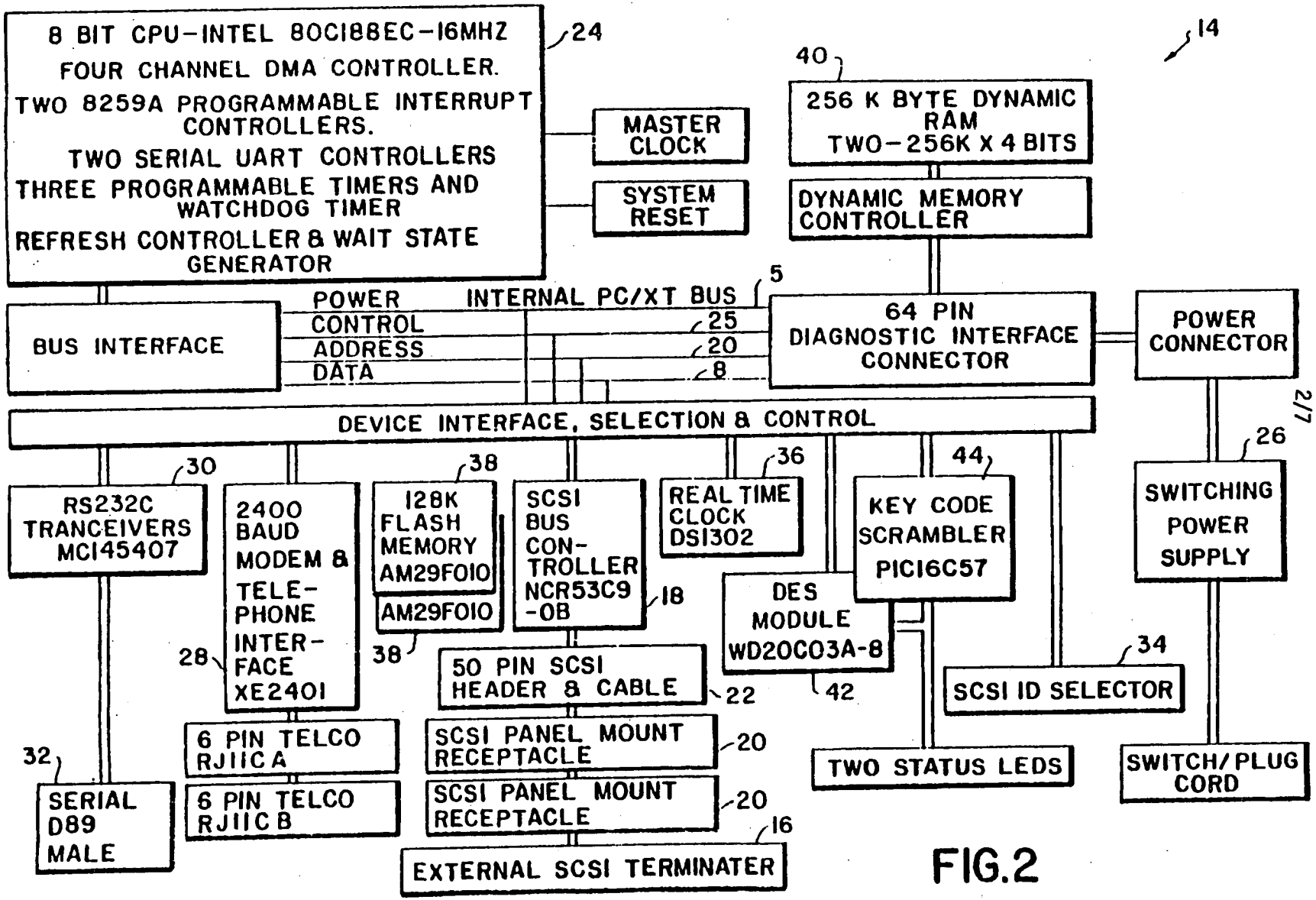

8 BIT CPU-INTEL 80C188EC-16MHZ
FOUR CHANNEL DMA CONTROLLER.
TWO 8259A PROGRAMMABLE INTERRUPT CONTROLLERS.
TWO SERIAL UART CONTROLLERS
THREE PROGRAMMABLE TIMERS AND WATCHDOG TIMER
REFRESH CONTROLLER & WAIT STATE GENERATOR
24
MASTER CLOCK
SYSTEM RESET
14
40
256 K BYTE DYNAMIC RAM TWO-256K X 4 BITS
DYNAMIC MEMORY CONTROLLER
5
INTERNAL PC/XT BUS
POWER
CONTROL
ADDRESS
DATA
25
20
8
BUS INTERFACE
64 PIN DIAGNOSTIC INTERFACE CONNECTOR
POWER CONNECTOR
DEVICE INTERFACE, SELECTION & CONTROL
30
RS232C TRANCEIVERS MC145407
2400 BAUD MODEM & TELE-PHONE INTER-FACE XE2401
28
38
128K FLASH MEMORY AM29F010
AM29F010
38
SCSI BUS CON-TROLLER NCR53C9-0B
18
36
REAL TIME CLOCK DS1302
44
KEY CODE SCRAMBLER PIC16C57
DES MODULE WD20C03A-8
42
26
SWITCHING POWER SUPPLY
34
SCSI ID SELECTOR
50 PIN SCSI HEADER & CABLE
22
6 PIN TELCO RJ11C A
6 PIN TELCO RJ11C B
SCSI PANEL MOUNT RECEPTACLE
20
SCSI PANEL MOUNT RECEPTACLE
20
32
SERIAL D89 MALE
16
EXTERNAL SCSI TERMINATER
TWO STATUS LEDS
SWITCH/PLUG CORD

FIG.2

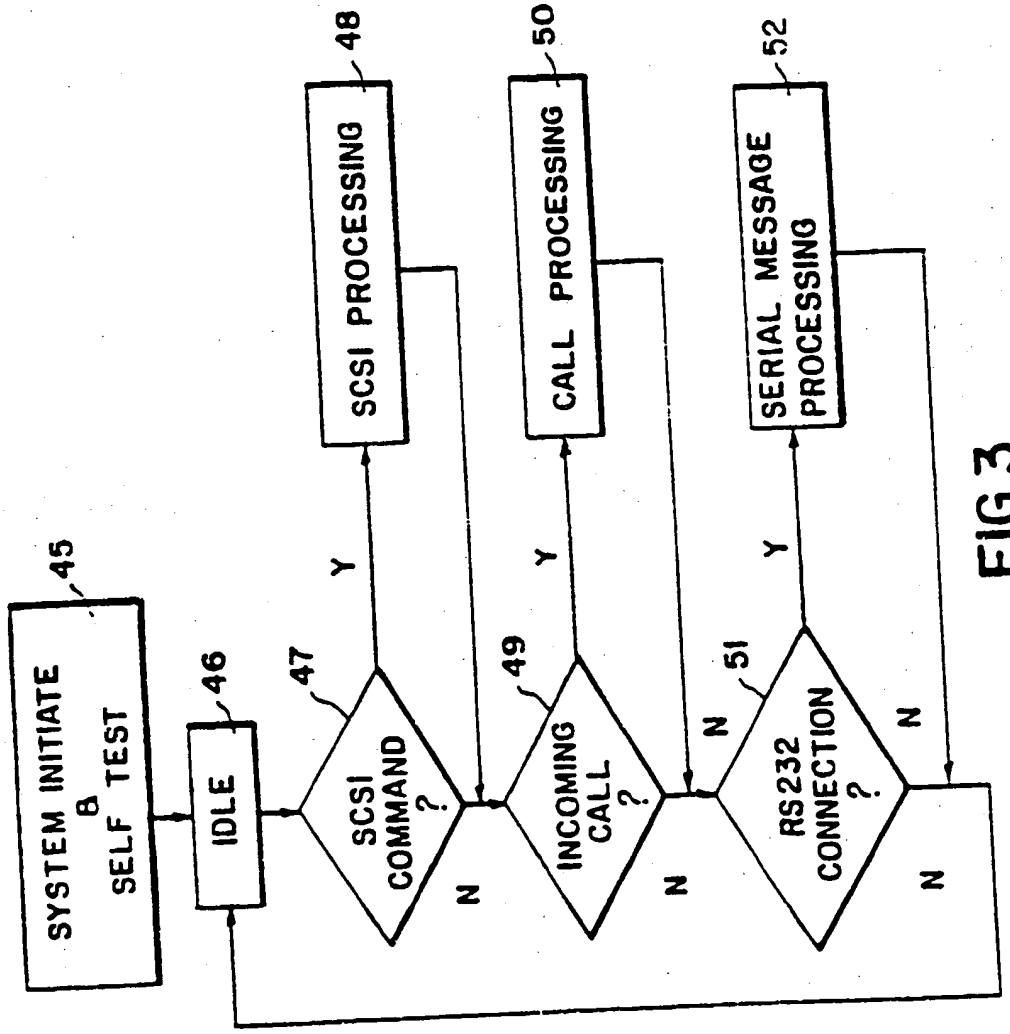

SYSTEM INITIATE & SELF TEST
45
IDLE
46
SCSI COMMAND ?
47
Y
N
SCSI PROCESSING
48
INCOMING CALL ?
49
Y
N
CALL PROCESSING
50
RS232 CONNECTION ?
51
Y
N
SERIAL MESSAGE PROCESSING
52

FIG.3

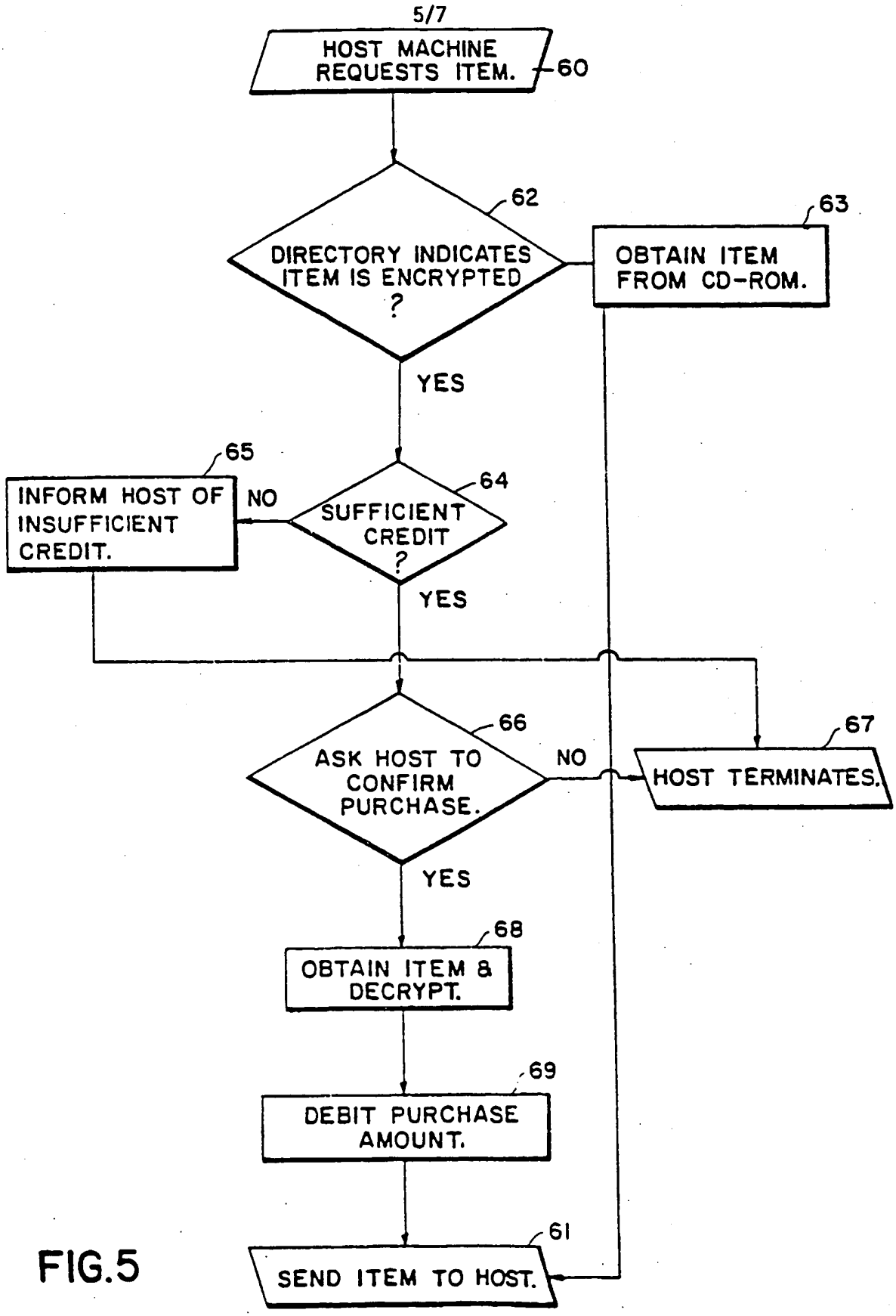

HOST MACHINE REQUESTS ITEM.
60
62
DIRECTORY INDICATES ITEM IS ENCRYPTED ?
63
OBTAIN ITEM FROM CD-ROM.
YES
65
INFORM HOST OF INSUFFICIENT CREDIT.
NO
64
SUFFICIENT CREDIT ?
YES
66
ASK HOST TO CONFIRM PURCHASE.
NO
67
HOST TERMINATES.
YES
68
OBTAIN ITEM & DECRYPT.
69
DEBIT PURCHASE AMOUNT.
61
SEND ITEM TO HOST.

FIG.5

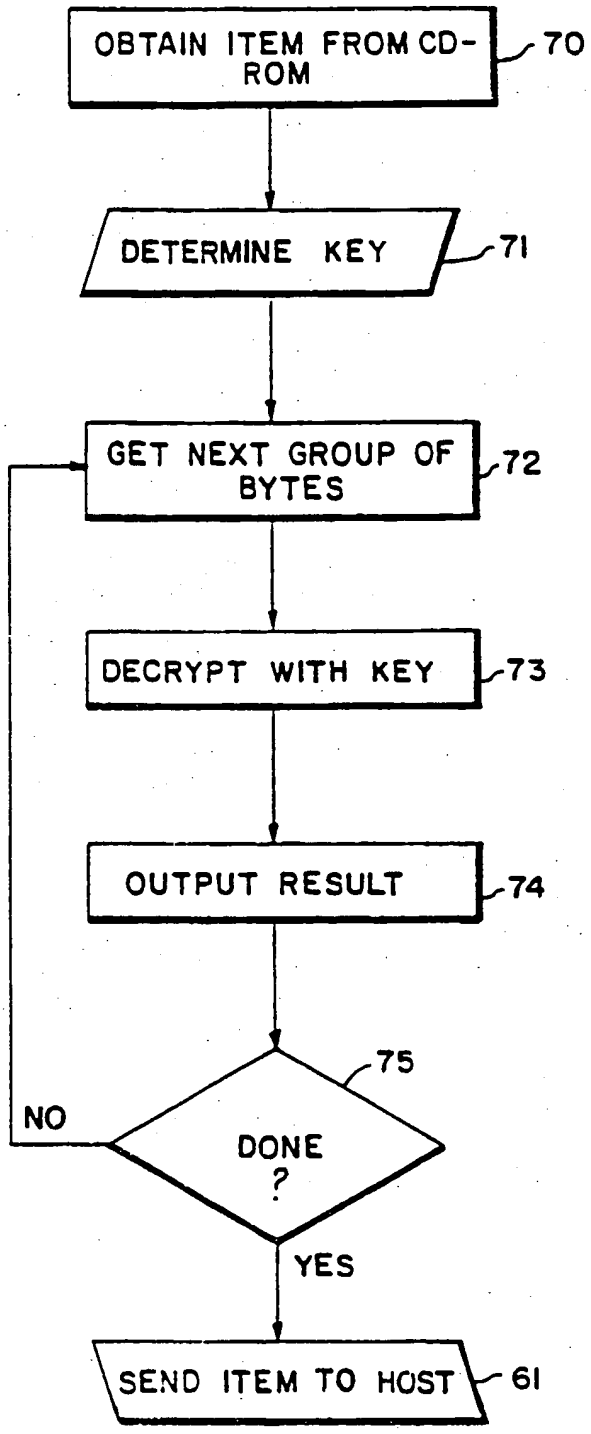

OBTAIN ITEM FROM CD-ROM
70
DETERMINE KEY
71
GET NEXT GROUP OF BYTES
72
DECRYPT WITH KEY
73
OUTPUT RESULT
74
75
NO
DONE ?
YES
SEND ITEM TO HOST
61

FIG.6

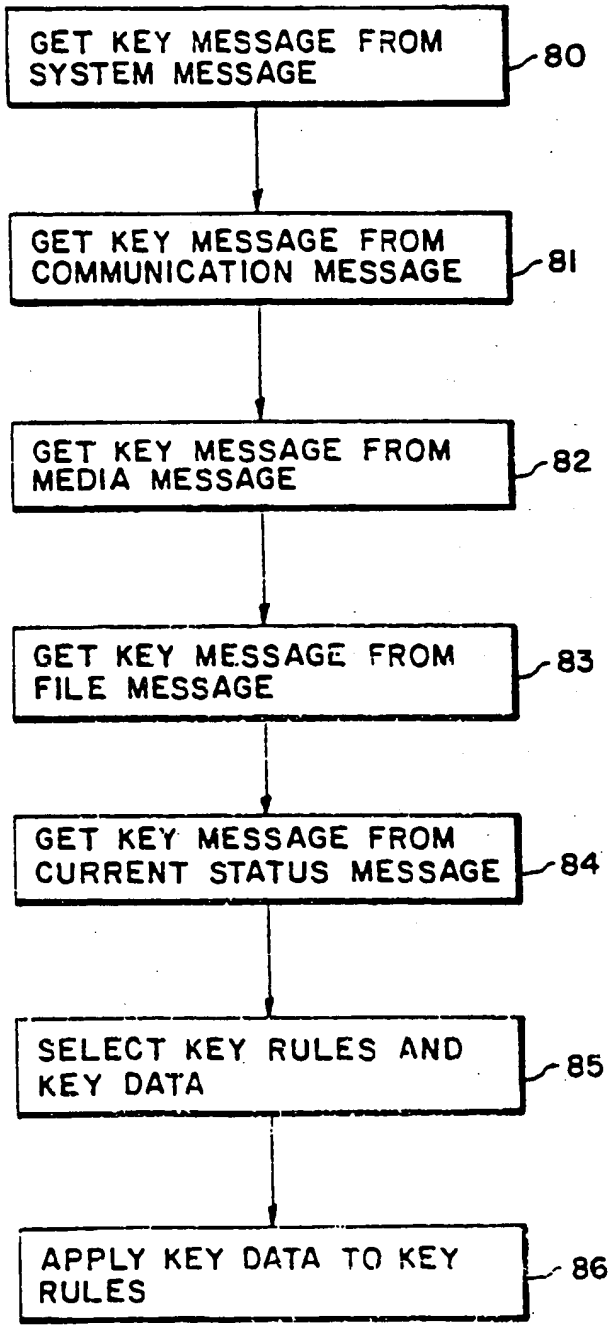

GET KEY MESSAGE FROM SYSTEM MESSAGE
80
GET KEY MESSAGE FROM COMMUNICATION MESSAGE
81
GET KEY MESSAGE FROM MEDIA MESSAGE
82
GET KEY MESSAGE FROM FILE MESSAGE
83
GET KEY MESSAGE FROM CURRENT STATUS MESSAGE
84
SELECT KEY RULES AND KEY DATA
85
APPLY KEY DATA TO KEY RULES
86

FIG.7

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 95/01740

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00 G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO,A,88 02960 (PERSONAL LIBRARY SOFTWARE INC) 21 April 1988	1,13,19
A	see the whole document	2-12, 14-18
A	EP,A,0 561 685 (FUJITSU LIMITED) 22 September 1993 see column 3, line 29 - column 6, line 8 see column 11, line 13 - line 54; figures 2,10C	1-18
A	WO,A,90 02382 (INDATA CORP) 8 March 1990 see page 30, paragraph 3 - page 43, paragraph 2; figures 5-13	1-21
A	EP,A,0 417 447 (IBM) 20 March 1991 see column 2, line 31 - column 3, line 15; figures 1,2	22,23

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 June 1995	04.07.95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Moens, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inten nal Application No
PCT/US 95/01740

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A-8802960	21-04-88	EP-A-	0329681	30-08-89
		US-A-	4977594	11-12-90
		US-A-	5410598	25-04-95
		US-A-	5050213	17-09-91
		US-A-	4827508	02-05-89
		US-A-	5272750	21-12-93
EP-A-561685	22-09-93	JP-A-	5257816	08-10-93
		US-A-	5392351	21-02-95
WO-A-9002382	08-03-90	AU-A-	4188289	23-03-90
		EP-A-	0472521	04-03-92
		US-A-	5247575	21-09-93
EP-A-417447	20-03-91	US-A-	5027397	25-06-91
		JP-A-	3105538	02-05-91
		US-A-	5159629	27-10-92